Quelques calculs de sommes de Gauss

Bruno Kahn

QUELQUES CALCULS DE SOMMES DE GAUSS

par

Bruno Kahn

Résumé. — On remarque que l'action galoisienne sur les constantes locales associées aux représentations galoisiennes d'un corps local fournit des renseignements sur leur nature arithmétique, permettant notamment de borner leur ordre quand ce sont des racines de l'unité. Elle fournit aussi des renseignments sur l'effet des opérations d'Adams sur ces constantes.

Abstract. — We observe that the Galois action on local constants associated to Galois representations of a local field yields information on their arithmetic nature, for example provides an upper bound to their order when they are roots of unity. It also yields information on the effect of Adams operations on these constants.

À Paulo Ribenboïm

Introduction

Les constantes locales, ou facteurs epsilon locaux, associés à une représentation galoisienne complexe d'un corps local, ont été relativement peu étudiés pour eux-mêmes. Rappelons qu'il s'agit d'une décomposition canonique de la constante de l'équation fonctionnelle des fonctions L d'Artin en produits de facteurs locaux, généralisant la décomposition obtenue à partir de la thèse de Tate [**14**] dans le cas abélien.

Plus précisément, si K est un corps global, la fonction L d'Artin complétée $\Lambda(\rho, s)$ associée à une représentation complexe ρ du groupe de Galois absolu de K admet (d'après Artin et Brauer) un prolongement

méromorphe au plan complexe et une équation fonctionnelle de la forme

$$\Lambda(\rho, 1-s) = W(\rho)\Lambda(\rho^*, s)$$

où ρ^* est la représentation duale de ρ et $W(\rho)$ est un nombre complexe de module 1 [**12**, p. 14]. De plus $W(\rho) \in \mathbf{Q}^{\mathrm{ab}}$, la clôture cyclotomique de $\mathbf{Q}$.

Lorsque ρ est de degré 1, le corps de classes et la thèse de Tate donnent une décomposition [**14**, p. 346]

$$W(\rho) = \prod_v W(\rho_v) \tag{1}$$

dans laquelle v décrit l'ensemble des places de K et ρ_v est la restriction de ρ au groupe de décomposition en v. Le nombre complexe $W(\rho_v)$ ne dépend que de ρ_v, est de module 1 et vaut 1 si ρ est non ramifié en v.

Langlands a démontré que la décomposition (1) s'étendait au cas non abélien. Sa démonstration, non publiée, est résumée dans un manuscrit non publié de Helmut Koch [**10**]. Une autre démonstration en a été donnée par Deligne [**1**] ; une variante de celle-ci apparaît au §2 de [**15**], qui me servira de référence principale dans cette note. Dans le cas de caractéristique positive, une troisième preuve est donnée par Laumon dans [**11**].

Rappelons que, si maintenant K est un corps local, la fonction $\rho \mapsto W(\rho)$ est caractérisée par les axiomes suivants

(i) *Additivité* : $W(\rho + \rho') = W(\rho)W(\rho')$.

(ii) *Inductivité en degré* 0 : si L/K est une extension finie, et si ρ est un caractère virtuel du groupe de Galois absolu G_L, de degré 0, alors $W(\mathrm{Ind}_{G_L}^{G_K} \rho) = W(\rho)$.

(iii) *Normalisation* : Si $\deg \rho = 1$, $W(\rho)$ est donné par la formule de [**14**, p. 322] via le corps de classes local.

Voici, à ma connaissance, ce qui apparaît dans la littérature sur les nombres $W(\rho)$:

1. Une étude détaillée de $W(\rho)$ est faite par Fröhlich dans [**5**] lorsque ρ est modérément ramifiée.
2. Si ρ est irréductible et sauvagement ramifiée (c'est-à-dire que l'exposant de son conducteur d'Artin est > 1), $W(\rho)$ est une racine de l'unité [**15**, cor. 4]. Cela résulte du cas de degré 1, où le résultat est dû à Lamprecht et Dwork (ibid., cor. 1). Dans [**6**, 1.4], Gérardin et

Kutzko donnent de ce cas particulier une preuve plus explicite que celle figurant dans [**15**].

3. Si ρ est orthogonale, virtuelle de degré 0 et de déterminant 1, $W(\rho)^2 = 1$; dans [**2**], Deligne donne la formule
$$W(\rho) = (-1)^{w_2(\rho)}$$
où $w_2(\rho)$ est la *deuxième classe de Stiefel-Whitney* de ρ.
4. Si ρ est symplectique, virtuelle de degré 0 et de déterminant 1, on a encore $W(\rho)^2 = 1$; le signe de $W(\rho)$ est intimement lié à la structure de module galoisien de l'anneau des entiers de L, où ρ se factorise par $Gal(L/K)$ (Fröhlich, Taylor...voir par exemple [**4**]).
5. Dans [**3**], Deligne et Henniart étudient comment $W(\rho)$ varie quand on tord ρ par une représentation pas trop ramifiée. Ils posent aussi une question relative à la trivialité de W sur certains produits tensoriels de représentations (question 4.10), et y répondent positivement dans certains cas particuliers.
6. Dans [**7**], Henniart étend la version de Gérardin-Kutzko du théorème de Lamprecht et Dwork mentionné ci-dessus à certaines représentations galoisiennes "sauvages homogènes". Pour une telle représentation ρ, il obtient une décomposition du type
$$W(\rho) \equiv \det_\rho(g_\rho)^{-1} G(g_\rho)^{\deg \rho} \pmod{\mu} \tag{2}$$
où μ est le groupe des racines p-primaires de l'unité (p = caractéristique résiduelle), g_ρ est essentiellement un élément de K^* attaché à ρ et $G(g_\rho)$ est une somme de Gauss quadratique attachée à g_ρ. Par convention $G(g_\rho) = 1$ si $p = 2$, et $G(g_\rho)$ est une racine 4-ième de l'unité si $p > 2$.
7. Dans [**16**] et [**17**], Volf résoud affirmativement certains cas de [**3**, qu. 4.10].

Dans cette note, je m'intéresse principalement à la partie *p-primaire* de $W(\rho)$, lorsque ce nombre est une racine de l'unité, où p est la caractéristique résiduelle. L'observation centrale est très simple : en étudiant l'action de $Gal(\mathbf{Q}^{\mathrm{ab}}/\mathbf{Q})$ sur $W(\rho)$, on peut borner l'ordre de cette partie p-primaire en fonction du corps de définition de ρ. Voir proposition 1 et ses corollaires. Les calculs indiquent en fait que le comportement galoisien est très différent sur trois facteurs (canoniques ?) de $W(\rho)$ généralisant (2).

Une première version de ces résultats a été obtenue en 1986 [**9**]. Ils ont ensuite été raffinés au cours des années 80/90, suivant notamment des suggestions de Guy Henniart, mais je ne les ai jamais soumis à publication. J'espère qu'il n'est pas trop tardif de le faire maintenant : je remercie Claude Lévesque pour son amicale insistance sur ce point. Ce texte est plus ou moins le contenu des notes d'une série d'exposés que j'ai faits à l'Université McMaster en 1989 ou 1991, avec des ajouts pour $p = 2$.

Il est tentant de se demander si ces calculs éclairent la question 4.10 de [**3**]. J'ai jugé plus prudent de m'en abstenir ici, pour ne pas retarder encore plus la rédaction.

Notations. — K est un corps local non archimédien, de caractéristique 0 et de caractéristique résiduelle p. Son corps résiduel est $\mathbf{F}_q$. Selon Langlands et Deligne, on associe à une représentation complexe ρ du groupe de Weil de K un *facteur epsilon* $\varepsilon(\rho, \psi, dx, s)$, dépendant également d'un caractère additif ψ de K, d'une mesure de Haar dx sur K et d'une variable complexe s. Comme dans [**15**], on choisit pour ψ le caractère additif standard :

$$\psi_K : K \xrightarrow{\mathrm{Tr}_{K/\mathbf{Q}_p}} \mathbf{Q}_p \longrightarrow \mathbf{Q}_p/\mathbf{Z}_p \hookrightarrow \mathbf{Q}/\mathbf{Z} \xrightarrow{\exp 2\pi i -} \mathbf{C}^*$$

pour dx la mesure de Haar autoduale pour ψ, et on pose

$$W(\rho) = \varepsilon(\rho, \psi_K, dx, 1/2).$$

Ces normalisations semblent importantes au moins pour certains calculs, notamment au §4.

Je ne considérerai que des représentations galoisiennes, c'est-à-dire se prolongeant au groupe de Galois absolu de K : cela ne restreint pas vraiment la généralité puisqu'une représentation du groupe de Weil s'obtient par torsion à partir d'une représentation galoisienne.

On note $\mathfrak{f}(\rho)$ le conducteur de ρ et $c(\rho)$ son exposant. On note $\Gamma = Gal(\mathbf{Q}^{\mathrm{ab}}/\mathbf{Q})$, $\kappa : \Gamma \xrightarrow{\sim} \hat{\mathbf{Z}}^*$ le caractère cyclotomique et $\kappa_p : \Gamma \to \mathbf{Z}_p^*$ sa composante p-primaire. On note $E = \mathbf{Q}(\rho) \subset \mathbf{Q}^{\mathrm{ab}}$ le corps engendré par les valeurs du caractère de ρ et $\Gamma_E = Gal(\mathbf{Q}^{\mathrm{ab}}/E)$. Si $a, b \in K^*$, on note $(a, b) \in \{\pm 1\}$ leur symbole de Hilbert.

1. Remarques sur une racine 4-ième de l'unité

Supposons $p > 2$. On peut se demander s'il existe une fonction $\rho \mapsto \iota(\rho)$, à valeurs dans les racines 4-ièmes de l'unité, coïncidant avec $G(g_\rho)^{\deg \rho}$ dans le cas de (2) et vérifiant les conditions (i) et (ii) de l'introduction. Je n'étudierai pas ce problème ici, mais me contenterai de deux remarques :

Lemme 1. — *a) Dans* (2)*, on a*

$$G(g_\rho)^{2\deg\rho} = (-1, \mathfrak{f}(\rho))$$

où $\mathfrak{f}(\rho)$ *désigne un générateur quelconque du conducteur de* ρ*. Cette fonction vérifie les conditions* (i) *et* (ii) *de l'introduction.*
b) Soit K_0 *un corps de nombres, et soit* ρ *une représentation galoisienne complexe de* G_{K_0}*. Pour toute place* v *de* K_0*, notons* ρ_v *la restriction de* ρ *au groupe de décomposition en* v*. Alors le produit*

$$\prod_{v \text{ finie impaire}} (-1, \mathfrak{f}(\rho_v))_v$$

ne dépend pas que des composantes dyadiques et archimédiennes de ρ*.*

Démonstration. — a) résulte facilement de la définition de $G(g_\rho)$ et de g_ρ [**7**, §§2, 4]. La seconde affirmation est évidente.

Pour b), il suffit de donner un exemple. On prend $K_0 = \mathbf{Q}$; soit l un nombre premier impair, et soient p_1, p_2 deux nombres premiers vérifiant

(i) $p_1 \equiv p_2 \equiv 1 \pmod{l}$;

(ii) $l \mid \dfrac{p_i - 1}{d_i}$, où d_i est l'ordre de 2 dans $\mathbf{F}_{p_i}^*$;

(iii) $p_1 \equiv 1 \pmod 4$, $p_2 \equiv -1 \pmod 4$.

Pour $i = 1, 2$, soit χ_i un caractère de Dirichlet $\pmod{p_i}$ d'ordre l : leur existence est assurée par (i). Comme l est impair, χ_1 et χ_2 sont triviaux à l'infini, et (ii) implique qu'ils sont aussi triviaux en 2. D'autre part, $(-1, \mathfrak{f}(\chi_i))_p = 1$ si $p \neq p_i$, et (iii) implique que $(-1, \mathfrak{f}(\chi_1))_{p_1} = 1$, $(-1, \mathfrak{f}(\chi_2))_{p_2} = -1$.

Un exemple minimal est $l = 3$, $p_1 = 109$, $p_2 = 31$. □

Le sens du lemme 1 a) est que l'obstruction à étendre $\rho \mapsto G(g_\rho)^{\deg\rho}$ dans le style de l'introduction disparaît quand on l'élève au carré. Le lemme 1 b) suggère qu'on ne peut guère attendre une preuve d'existence de cette extension par la méthode de Deligne [**1**].

Pour la suite je me contenterai d'une version de $\iota(\rho)$ au signe près. Une telle fonction est facile à exhiber : on peut prendre

$$\iota(\rho) = i^{\left(\frac{N(\mathfrak{f}(\rho))-1}{2}\right)^2}.$$

Définition 1. — Si $p > 2$,

$$W^*(\rho) = \iota(\rho)W(\rho). \tag{3}$$

Si $p = 2$, $W^*(\rho) = W(\rho)$.

L'inconvénient de ce choix de $\iota(\rho)$ est qu'il est invariant par l'action de Galois : ce n'est pas le cas de l'invariant $G(g_\rho)^{\deg \rho}$ de Henniart. On peut espérer qu'une réponse positive à la question ci-dessus permettrait de se débarrasser complètement des désagréables symboles de Hilbert polluant les formules ci-dessous.

2. Action galoisienne sur $W^*(\rho)$

Toute représentation galoisienne complexe ρ est définie sur un corps cyclotomique ; le groupe de Galois $\Gamma = Gal(\mathbf{Q}^{\mathrm{ab}}/\mathbf{Q})$ opère donc sur [le caractère de] ρ, ainsi que sur $W(\rho) \in \mathbf{Q}^{\mathrm{ab}}$.

Si p est un nombre premier impair, posons $p^* = (-1)^{\frac{p-1}{2}}p$, de sorte que $\mathbf{Q}(\sqrt{p^*}) \subset \mathbf{Q}(\mu_p)$. Si $p = 2$, posons $p^* = p$: on a $\mathbf{Q}(\sqrt{2}) \subset \mathbf{Q}(\mu_8)$. Le lemme suivant se vérifie facilement (pour $p = 2$, utiliser la relation $(2, -1) = 1$) :

Lemme 2. — *Pour tout nombre premier p et tout $\sigma \in \Gamma$, on a*

$$\sqrt{p^*}^{\sigma-1} = (p, \kappa_p(\sigma))$$

(symbole de Hilbert calculé dans $\mathbf{Q}_p$). □

On en déduit :

Proposition 1. — *Soit $\sigma \in \Gamma$. Alors*

$$W^*(\rho)^\sigma = W^*(\rho^\sigma)\det_\rho(\kappa_p(\sigma))^\sigma(N\mathfrak{f}(\rho), \kappa_p(\sigma))$$

où $\kappa_p(\sigma) \in \mathbf{Z}_p^*$ est le caractère p-cyclotomique de σ et $\det_\rho$ est la représentation déterminant de ρ, vue comme caractère multiplicatif via le corps de classes local.

Démonstration. — C'est une reformulation du théorème de Fröhlich [**12**, p. 43, cor. 5.2]. Avoir remplacé $W(\rho)$ par $W^*(\rho)$ donne une formule légèrement plus propre. □

Corollaire 1. — *Soit $E \subset \mathbf{Q}^{\mathrm{ab}}$ le corps engendré par les valeurs du caractère de ρ. Notons p^n le nombre exact de racines p-primaires de l'unité contenues dans E.*
a) Si $p > 2$ et $n > 0$, $W^*(\rho) \in \mu_{p^{n+1}} E^*$.
b) Si $p > 2$ et $n = 0$, $W^*(\rho) \in E(\mu_p)^*$ et $W^*(\rho)^{2d} \in E^*$, où $d = \mathrm{pgcd}(|\mu_{p-1} \cap E|, [E(\mu_p) : E])$.
c) Si $p = 2$ et $n \geq 2$, $W^*(\rho) \in \mu_{2^{n+2}} E^*$.
d) Si $p = 2$ et $n = 1$, $W^*(\rho) \in E(\mu_8)^*$ et $W^*(\rho)^2 \in E^*$.

Démonstration. — Soit $\sigma \in \Gamma_E := Gal(\mathbf{Q}^{\mathrm{ab}}/E)$. Comme $\det_\rho$ prend ses valeurs dans E, on a :

$$W^*(\rho)^{\sigma-1} = \det_\rho(\kappa_p(\sigma))(N\mathfrak{f}(\rho), \kappa_p(\sigma)).$$

a) L'hypothèse implique que $\kappa_p(\sigma) \equiv 1 \pmod{p^n}$.

Si $p > 2$, $\kappa_p(\sigma)$ est un carré et le symbole de Hilbert vaut 1. De plus, $\det_\rho(\kappa_p(\sigma)) \in \mu_p$: en effet $\det_\rho(1 + p\mathbf{Z}_p) \subset \mu_{p^n}$ et $1 + p^n\mathbf{Z}_p = (1 + p\mathbf{Z}_p)^{p^{n-1}}$. On trouve donc que $W^*(\rho)^{\sigma-1} \in \mu_p$, et $W^*(\rho)^{\sigma-1} = 1$ si $\kappa_p(\sigma) \in 1 + p^{n+1}\mathbf{Z}_p$. Il en résulte que $W^*(\rho) \in E(\mu_{p^{n+1}})$ et $W^*(\rho)^p \in E$, donc que $W^*(\rho) \in \mu_{p^{n+1}} E^*$.

b) On a $\det_\rho(u) = 1$ et $(p, u) = 1$ si $u \in 1 + p\mathbf{Z}_p$: ceci montre que $W^*(\rho) \in E(\mu_p)$. Posons maintenant $d_1 = |\mu_{p-1} \cap E|$, $d_2 = [E(\mu_p) : E]$ et $d = \mathrm{pgcd}(d_1, d_2)$. Alors $\det_\rho(\kappa_p(\sigma)) \in \mu_d$ pour tout $\sigma \in \Gamma_E$, puisque $\sigma^{d_2} \in \Gamma_{E(\mu_p)}$. De plus, on voit que $W^*(\rho)^d \in E$ si d est pair et $W^*(\rho)^{2d} \in E$ si d est impair.

c) Si $p = 2$, le raisonnement de a) reste valable tant que $n \geq 3$ ($(\mathbf{Z}_2^*)^{2^{n-2}} = 1 + 2^n\mathbf{Z}_2 \Rightarrow \det \rho(1 + 2^n\mathbf{Z}_2) \subset \mu_4$), et même pour $n = 2$ (alors $\det \rho(u) \in \mu_4$ pour tout $u \in \mathbf{Z}_2^*$).

d) Même calcul que précédemment. □

Corollaire 2. — *Gardons les notations du corollaire 1, et supposons que $\det_\rho$ soit trivial. Alors $W^*(\rho) \in E^*$, sauf si*

(i) *$p > 2$, $n = 0$ et $N\mathfrak{f}(\rho)$ n'est pas un carré ; alors $W^*(\rho) \in \sqrt{p^*}E^*$.*

(ii) *$p = 2$, $n = 2$ et $N\mathfrak{f}(\rho)$ n'est pas un carré ; alors $W^*(\rho) \in \mu_8 E^*$.*

(iii) *$p = 2$, $n = 1$.*

Démonstration. — On reprend la démonstration du corollaire 1. □

Remarque 1. — Supposons ρ somme de représentations homogènes au sens de [**7**, §4]. Si $p > 2$, on a nécessairement $n > 0$: en effet, la restriction d'une composante irréductible au dernier saut de ramification est une somme de caractères de degré 1, tous égaux entre eux, sur un p-groupe (*loc.cit.*). Lorsque $p = 2$ il existe des caractères quadratiques sauvages, par exemple pour $K = \mathbf{Q}_2$ celui donné par l'extension $K(\sqrt{2})/K$.

Corollaire 3. — *Gardons les notations du corollaire 1, et supposons que $W^*(\rho)$ soit une racine de l'unité. Soit m le nombre de racines de l'unité de E. Alors*

$$W^*(\rho)^m = \begin{cases} 1 & \text{si } p \nmid m \\ \det_\rho(1+m) & \text{si } p \text{ est impair et } p \mid m \\ \det_\rho(1+m) & \text{si } p = 2 \text{ et } 8 \mid m \\ \det_\rho(1+m)(-1)^{v_2(N\mathfrak{f}(\rho))} & \text{si } p = 2 \text{ et } 8 \nmid m. \end{cases}$$

Démonstration. — Supposons d'abord $p > 2$. D'après le corollaire 1 a) et b), on a $W^*(\rho) \in \mu_{pm}$.

Si $p \nmid m$, on a aussi $W^*(\rho)^{2d} \in \mu_m$, où $2d$ est premier à p. Donc $W^*(\rho) \in \mu_m$, d'où l'énoncé.

Supposons $p \mid m$. L'image de $\kappa(\Gamma_E)$ dans $(\mathbf{Z}/m)^*$ (*resp.* dans $(\mathbf{Z}/pm)^*$) est triviale (*resp.* non triviale) puisque $\mu_m \subset E$ (*resp.* $\mu_{pm} \not\subset E$). Comme $\mathrm{Ker}\,((\mathbf{Z}/pm)^* \to (\mathbf{Z}/m)^*)$ est cyclique d'ordre p engendré par $1+m$, on peut choisir $\sigma \in \Gamma_E$ tel que $W^*(\rho)^\sigma = W^*(\rho)^{1+m}$ et $\kappa_p(\sigma) = 1+m$. En particulier $\kappa_p(\sigma) \equiv 1 \pmod p$, donc $\kappa_p(\sigma)$ est un carré. Alors l'énoncé découle de la proposition 1.

Supposons maintenant $p = 2$. On peut encore choisir σ comme ci-dessus. D'après le corollaire 1 a), c) et d), on a $W^*(\rho) \in \mu_{4m}$. Soit $n = v_2(m)$. Si $n \geq 3$, $1+m \equiv 1 \pmod 8$ est un carré dans $\mathbf{Q}_2$, donc le même calcul que ci-dessus est valable. Si $n = 2$ (*resp.* $n = 1$), $1+m \equiv 5 \pmod 8$ (*resp.* $1+m \equiv 3 \pmod 8$) : dans les deux cas on a $(N\mathfrak{f}(\rho), 1+m)_2 = (-1)^{v_2(N\mathfrak{f}(\rho))}$, d'où la formule dans ces cas. □

3. Opérations d'Adams

3.1. Rappel. — Soit G un groupe fini, et notons $R(G)$ l'anneau des représentations complexes de G. Si $\rho \in R(G)$ est de caractère χ et si $k \in \mathbf{Z}$, on note $\Psi^k\chi$ la fonction centrale définie par

$$\Psi^k\chi(g) = \chi(g^k).$$

On démontre (par exemple [**13**, §9.1, ex. 3]) que c'est le caractère d'une représentation, notée $\Psi^k\rho$.

Supposons maintenant k premier à l'ordre de G. Alors Ψ^k ne dépend que de k modulo e, où e est l'exposant de G. On obtient ainsi une action de $(\mathbf{Z}/e)^*$ sur $R(G)$.

D'autre part, les caractères de G prennent leurs valeurs dans $F = \mathbf{Q}(\mu_e)$. On a donc aussi une action de $Gal(F/\mathbf{Q})$ sur $R(G)$, et

Lemme 3. — *Soit $\kappa : Gal(F/\mathbf{Q}) \xrightarrow{\sim} (\mathbf{Z}/e)^*$ le caractère cyclotomique. Pour tout $\rho \in R(G)$ et tout $\sigma \in Gal(F/\mathbf{Q})$, on a $\rho^\sigma = \Psi^{\kappa(\sigma)}\rho$.* □

Ceci montre que $\Psi^k\rho$ ne dépend que de l'image de k dans $\hat{\mathbf{Z}}^*/\kappa(\Gamma_E)$, où $E = \mathbf{Q}(\rho)$.

3.2. Action des opérations d'Adams sur les constantes locales. — En combinant le lemme 3 et la proposition 1, on obtient :

Proposition 2. — *Soit ρ une représentation galoisienne complexe de K. Soit L/K une extension finie galoisienne par laquelle se factorise ρ, et soit k un entier premier à $d = [L : K]$. Notons d_p la plus grande puissance de p divisant d. Alors*

$$W^*(\Psi^k\rho) = W^*(\rho)^\sigma \det_\rho(k_p)^{-k}(N\mathfrak{f}(\rho), k_p)$$

où $\sigma \in Gal(\mathbf{Q}(\mu_d)/\mathbf{Q})$ est un élément de caractère cyclotomique congru à k modulo d, et k_p est la projection de k dans $(\mathbf{Z}/d_p)^*$. □

On en déduit le corollaire suivant, qui précise le corollaire 3 :

Corollaire 4. — *Gardons les notations de la proposition 2 et supposons que $W^*(\rho)$ soit une racine de l'unité. Si k est premier à pd (en particulier si p divise d), on a*

$$W^*(\Psi^k\rho) = W^*(\rho)^k \det_\rho(k_p)^{-k}(N\mathfrak{f}(\rho), k_p).$$

En particulier, si $k \in \kappa(\Gamma_E)$, on a

$$W^*(\rho)^{k-1} = \det_\rho(k_p)(N\mathfrak{f}(\rho), k_p).$$

Voici un exemple amusant :

Corollaire 5. — *Dans le corollaire 4, supposons que $\mu_p \subset E$ mais $\mu_{p^2} \not\subset E$ (par exemple que ρ soit un caractère d'ordre p). Alors*

$$W^*(\Psi^k\rho) = W^*(\rho)^{k^p}(N\mathfrak{f}(\rho), k_p).$$

Démonstration. — L'hypothèse signifie que $\kappa_p(\Gamma_E) = 1 + p\mathbf{Z}_p$. En particulier $k_p^{p-1} \in \kappa_p(\Gamma_E)$ et d'après la seconde formule du corollaire 4 :

$$\det_\rho(k_p) = \det_\rho(k_p)^{1-p} = \det_\rho(k_p^{p-1})^{-1} = \left(W^*(\rho)^{k^{p-1}-1}\right)^{-1}.$$

En reportant dans la première formule du corollaire 4, on trouve

$$W^*(\Psi^k\rho) = W^*(\rho)^k \left(W^*(\rho)^{k^{p-1}-1}\right)^k (N\mathfrak{f}(\rho), k_p)$$
$$= W^*(\rho)^{k^p}(N\mathfrak{f}(\rho), k_p).$$

□

Remarque 2. — Si ρ est un caractère d'ordre p, la formule du corollaire 5 s'étend aux valeurs de k divisibles par p grâce au corollaire 3 (en posant $k_p = 1$). Ce genre de formule ne semble pas se généraliser à des caractères d'ordre p^2 (voir proposition 3).

Dans le numéro suivant on dira quelque chose sur l'action d'une opération d'Adams Ψ^k lorsque k divise l'ordre d'un groupe de définition de ρ dans le cas où $p > 2$ et K est absolument non ramifié, *cf.* corollaire 6.

4. Exemple : caractères logarithmiques

Dans [**6**], une exponentielle tronquée pointe le bout du nez (pour $p = 2$) ; elle apparaît explicitement dans [**3**] pour des raisons différentes. Nous allons utiliser ici un "vrai" logarithme.

Soient U le groupe des unités de K et U_1 le groupe des unités principales. Rappelons que la fonction logarithme converge sur U_1 et définit un homomorphisme continu

$$\log : U_1 \to K$$

de noyau les racines p-primaires de l'unité. Il est habituel (Iwasawa) de prolonger log en un homomorphisme sur K^* tout entier comme suit :

- $\log \zeta = 0$ si ζ est une racine de l'unité (cette condition est nécessaire) ;
- Soit $x \in K^*$. Si e est l'indice de ramification absolu de K, on a $x^e = p^n u$ avec $u \in U$ et $n \in \mathbf{Z}$. Alors $\log x = \frac{1}{e} \log u$.

Définition 2. — Soit $\alpha \in K$. Pour $x \in K^*$, on note

$$\chi_\alpha(x) = \psi_K(\alpha \log x).$$

C'est le *caractère logarithmique* attaché à α.

Tout caractère logarithmique est trivial sur les racines de l'unité et les puissances fractionnaires de p, et prend des valeurs p-primaires. Réciproquement :

Lemme 4. — *L'homomorphisme*

$$K \to \mathrm{Hom}(K^*/(\mu(K) + \langle p \rangle^{\mathbf{Q}} \cap K^*), \mu_{p^\infty}(\mathbf{C}))$$
$$\alpha \mapsto \chi_\alpha$$

est surjectif.

Démonstration. — C'est clair par dualité additive, puisque l'image de log est un sous-groupe ouvert de K. □

Malheureusement le noyau de $\alpha \mapsto \chi_\alpha$ dépend fortement de la ramification absolue de K. De même il est difficile d'évaluer le conducteur de χ_α en général. Pour ces raisons, je me limite maintenant au cas où $K/\mathbf{Q}_p$ est *non ramifié*.[1] On a alors un résultat assez agréable (en tout cas pour $p > 2$) :

Proposition 3. — *Supposons K non ramifié sur $\mathbf{Q}_p$.*
a) Pour $\alpha \in K$ on a $\chi_\alpha = 1 \iff |2\alpha| \leq p$. Si $|2\alpha| > p$, χ_α est de conducteur (α^{-1}) et d'ordre $|2\alpha|/p$.
b) Si $p > 2$, on a :

$$W(\chi_\alpha) = G(\alpha)\psi_K(\alpha(1 - \log \alpha))$$

où $G(\alpha)$ est la somme de Gauss quadratique normalisée de [**6**, p. 352] *(racine 4-ième de l'unité).*
b) Si $p = 2$ et $v(\alpha)$ est impair, on a

$$W(\chi_\alpha) = G(\chi_\alpha)\psi_K(\alpha(1 - \log \alpha))$$

où $G(\chi_\alpha)$ est la somme de Gauss quadratique normalisée de [**6**, p. 352] *(racine 8-ième de l'unité). Si $v(\alpha)$ est pair et ≤ -6, on a*

$$W(\chi_\alpha) = \psi_K(\alpha(1 - \log \alpha) - 2^{n-3}\alpha^{2F^{-1}-1})$$

où F est l'automorphisme de Frobenius absolu de K. (Voir la démonstration pour une formule dans le cas $v(\alpha) = -4$.)

1. Cette restriction n'est peut-être pas trop déraisonnable : étant donné la propriété d'inductivité de W, il suffit en fait d'étudier ces constantes dans le cas particulier $K = \mathbf{Q}_p$. C'est aussi raisonnable d'un point de vue motivique.

Démonstration. — a) découle du fait que $\log K^* = 2pO_K$ et que $v(\log(1+x)) = v(x)$ si $v(x) > \frac{e}{p-1}$ où e est l'indice de ramification absolu (ici, $e = 1$). Pour b) et c), on utilise la formule de [**6**, 1.4]

$$W(\chi_\alpha) = G(\chi_\alpha)\chi_\alpha(d)\psi_K(d^{-1})$$

pour un $d \in K$ tel que

$$\chi_\alpha(1+x) = \psi_K(d^{-1}x)$$

pour tout x tel que $v(x) \geq c - [c/2]$, où $c = v(\mathfrak{f}(\chi_\alpha))$ et $G(\chi_\alpha)$ est une racine 4-ième ou 8-ième de l'unité, valant 1 pour c pair (*cf.* [**15**, prop. 1]). Si $p > 2$, $G(\chi_\alpha)$ ne dépend que de d [**6**, p. 352].

Pour $p > 2$, on voit tout de suite que $d^{-1} = \alpha$ convient, et la formule résulte alors de la définition de χ_α. Pour $p = 2$, on s'intéresse à $\psi_K(\alpha \log(1+x))$. Écrivons $\alpha = a/2^n$ avec $a \in U$ et $n \geq 3$ (voir a)), d'où $c = n$. Pour $v(x) \geq n - [n/2]$ on a

$$\log(1+x) \equiv x - x^2/2 \pmod{2^n O_K}$$

et même $\log(1+x) \equiv x \pmod{2^n O_K}$ si n est impair. Dans ce cas, on peut choisir $d^{-1} = \alpha$ comme en b). Si n est pair, on écrit $x = 2^{n/2}u$; alors $x^2 = 2^n u^2$, donc

$$\begin{aligned}\psi_K(\alpha\frac{x^2}{2}) = \psi_K(\frac{a}{2^n}\frac{x^2}{2}) = \psi_K(\frac{a}{2}u^2) = \psi_K(\frac{a}{2}u^F)\\ = \psi_K(\frac{a^{F^{-1}}}{2}u) = \psi_K(\frac{a^{F^{-1}}}{2^{n/2+1}}x) = \psi_K(2^{n/2-1}\alpha^{F^{-1}}x)\end{aligned}$$

donc on peut choisir $d^{-1} = \alpha - 2^{n/2-1}\alpha^{F^{-1}}$, d'où

$$\chi_\alpha(d)\psi_K(d^{-1}) = \psi_K(-\alpha\log(\alpha - 2^{n/2-1}\alpha^{F^{-1}}) + \alpha - 2^{n/2-1}\alpha^{F^{-1}}).$$

Supposons maintenant $n \geq 6$. Alors on peut écrire

$$\begin{aligned}\log(\alpha - 2^{n/2-1}\alpha^{F^{-1}}) &= \log\alpha + \log(1 - 2^{n/2-1}\alpha^{F^{-1}-1})\\ &\equiv \log\alpha - 2^{n/2-1}\alpha^{F^{-1}-1} - 2^{n-3}\alpha^{2(F^{-1}-1)} \pmod{2^n O_K}\end{aligned}$$

d'où

$$\chi_\alpha(d)\psi_K(d^{-1}) = \psi_K(-\alpha(1-\log\alpha) - 2^{n-3}\alpha^{2F^{-1}-1})$$

comme souhaité. □

Supposons $p > 2$. Comme K ne contient pas de racines p-ièmes de l'unité, tout caractère sauvage χ de K^* s'écrit de manière unique comme produit d'un caractère modérément ramifié χ_0 et d'un caractère χ_α. Ceci

permet d'écrire une formule explicite pour $W(\chi)$ à partir de la proposition 3 : si $\chi = \chi_0\chi_\alpha$, on trouve

$$W(\chi) = \chi_0(\alpha)W(\chi_\alpha) = \chi_0(\alpha)G(\alpha)\psi_K(\alpha(1-\log\alpha))$$

cf. [**15**, p. 98 cor. 2].

Ainsi $W(\chi)$ se décompose canoniquement en produit de trois facteurs : une racine de l'unité $\chi_0(\alpha)$, une racine 4-ième de l'unité $G(\alpha)$ et une racine p-primaire de l'unité $\psi_K(\alpha(1-\log\alpha))$. Notons cette dernière $W_p(\chi)$.

Corollaire 6. — *Si $p > 2$, on a*

$$W_p(\chi^p) = W_p(\chi)^p$$

tant que χ^p est sauvage (c'est-à-dire que $\chi_\alpha^p \neq 1$). □

Corollaire 7. — *Soit $p > 2$.*
a) Supposons $\alpha = a/p^2$, où $a \in O_K$. Alors

$$W_p(\chi_\alpha) = \psi_K(\frac{a^p}{p^2}).$$

b) Pour $a_1, \ldots, a_p \in O_K$, on a

$$W_p((1-\chi_{a_1/p^2})\ldots(1-\chi_{a_p/p^2})) = \psi_K(\frac{a_1\ldots a_p}{p}).$$

c) Pour $a_1, \ldots, a_{p+1} \in O_K$, on a $W_p((1-\chi_{a_1/p^2})\ldots(1-\chi_{a_{p+1}/p^2})) = 1$.
d) Supposons $K = \mathbf{Q}_p$. Pour tout $n \geq 2$, on a $W_p((1-\chi_{1/p^n})^{p^{n-1}}) = \exp(2\pi i/p)$.

Démonstration. — a) La formule est vraie si a est divisible par p, puisqu'alors $\chi_\alpha = 1$. Sinon, écrivons $a = a_0(1+pu)$, avec $a_0^{q-1} = 1$ et $u \in O_K$. Alors $\log\alpha = pu + p^2v$ avec $v \in O_K$, et

$$W_p(\chi_\alpha) = \psi_K(\frac{a_0}{p^2}(1+pu)(1-pu+p^2v)) = \psi_K(\frac{a_0}{p^2}).$$

D'autre part $a_0 = a_0^q \equiv a^q \pmod{p^2}$, donc $\frac{a_0}{p^2} \equiv \frac{a^q}{p^2} \pmod{O_K}$. Mais soit F l'automorphisme de Frobenius de K. On a

$$a^p \equiv a^F \pmod{p}$$

d'où

$$a^{p^{n+1}} \equiv a^{p^nF} \pmod{p^{n+1}} \quad \forall n \geq 0$$

donc

$$\mathrm{Tr}_{K/\mathbf{Q}_p}(a^{p^{n+1}}) \equiv \mathrm{Tr}_{K/\mathbf{Q}_p}(a^{p^n}) \pmod{p^{n+1}} \quad \forall n \geq 0$$

et par récurrence

$$\mathrm{Tr}_{K/\mathbf{Q}_p}(a^q) \equiv \mathrm{Tr}_{K/\mathbf{Q}_p}(a^p) \pmod{p^2}$$

d'où finalement

$$\psi_K(\frac{a_0}{p^2}) = \psi_K(\frac{a^p}{p^2}).$$

b) résulte immédiatement de a) puisque la forme polaire de a^p est $p!a_1 \dots a_p$ et que $p! \equiv -1 \pmod{p}$ (théorème de Wilson). c) résulte aussi de a) (ou de b)).

Pour d), posons $\chi = \chi_{1/p^n}$. D'après la proposition 3, on a

$$W_p(\chi) = \psi_{\mathbf{Q}_p}(1/p^n) = \exp(2\pi i/p^n).$$

On écrit

$$(1-\chi)^{p^{n-1}} = \sum_{i=0}^{p^{n-1}} (-1)^i \binom{p^{n-1}}{i} \chi^i.$$

Pour $i = 0$ et $i = p^{n-1}$ on a $\chi^i = 1$, sinon $\chi^i \neq 1$; de plus $\chi^{p^{n-2}}$ est d'ordre p. Soient $i \in]0, p^{n-1}[$ et $t = v_p(i)$. Alors $v_p(\binom{p^{n-1}}{i}) = n-1-t$. Posons $i = p^t i_0$ et $\binom{p^{n-1}}{i} = p^{n-1-t}u$. Alors, en utilisant les corollaires 1 a), 5 et 6 :

$$W_p(\binom{p^{n-1}}{i}\chi^i) = W_p(\chi^i)^{\binom{p^{n-1}}{i}} = W_p(\chi^{p^t i_0})^{p^{n+1-t}u} = W_p(\chi^{p^{n-2}i_0})^{pu}$$

$$= W_p(\chi^{p^{n-2}})^{i_0^p pu} = W_p(\chi^{p^{n-2}})^{i_0 pu} = W_p(\chi)^{p^t i_0 p^{n-1-t}u} = W_p(\chi)^{i\binom{p^{n-1}}{i}}.$$

Par conséquent, $W_p((1-\chi)^{p^{n-1}}) = W_p(\chi)^A$, avec

$$A = \sum_{i=1}^{p^{n-1}-1} (-1)^i i \binom{p^{n-1}}{i}.$$

La somme $\sum_{i=1}^{p^{n-1}} (-1)^i i \binom{p^{n-1}}{i}$ est nulle, comme on le voit en prenant la dérivée de $(1-X)^{p^{n-1}}$. Donc $A = p^{n-1}$ et

$$W_p((1-\chi)^{p^{n-1}}) = W_p(\chi)^{p^{n-1}} = \exp(2\pi i/p).$$

□

Remarque 3. — a) Le corollaire 6 devient faux pour $p = 2$, même si χ est de la forme χ_α (voir proposition 3 c)). Dans le corollaire 7 a), le premier cas pour $p = 2$ serait $n = 3$. Les caractères χ_α sont alors quadratiques, donc $\alpha \mapsto W(\chi_\alpha)$ est une application quadratique d'après [**15**, p. 126, cor. 2]. J'ai donné une formule pour certains de ces caractères quadratiques dans [**8**, th. 2], à savoir

$$W(\rho_u) = i^{\mathrm{Tr}_{K/\mathbf{Q}_2}(\frac{u-1}{2}^2)}$$

pour $u \in 1 + 2O_K$, où $\rho_u(x) := (u, x)$ pour $x \in K^*$. Je renonce à la comparer à celle de la proposition 3 c), à commencer par déterminer u en fonction de $\alpha\ldots$

b) Le corollaire 7 a) donne aussi la formule suivante :

$$W_p((1 - \chi_{a_1/p^2})(1 - \chi_{a_2/p^2})) = \psi_K(p^{-1}\frac{(a_1 + a_2)^p - a_1^p - a_2^p}{p})$$

où on reconnaît la seconde composante du vecteur de Witt associé à $a_1 + a_2 \pmod p$.

Pour $n > 2$, je ne sais pas si la fonction $\chi \mapsto W_p(\chi)$ est polynomiale d'ordre p^{n-1} sur les caractères d'ordre $\leq p^{n-1}$: c'est suggéré par le corollaire 7 d). Ceci est à comparer avec le théorème 4.15 de [**3**].

Références

[1] P. Deligne *Les constantes des équations fonctionnelles des fonctions L*, *in* Modular Functions in one variable II, Lect. Notes in Math. **349**, Springer, 1973, 501–597.

[2] P. Deligne *Les constantes locales de l'équation fonctionnelle de la fonction L d'Artin d'une représentation orthogonale*, Invent. Math. **35** (1976), 299–316.

[3] P. Deligne, G. Henniart *Sur la variation, par torsion, des constantes locales d'équations fonctionnelles de fonctions L*, Invent. Math. **64** (1981), no. 1, 89–118.

[4] Ph. Cassou-Noguès, T. Chinburg, A. Fröhlich, M. J. Taylor *L-functions and Galois modules* (d'après des notes de D. Burns et N. P. Byott), London Math. Soc. Lect. Note Ser. **153**, *L*L-functions and arithmetic (Durham, 1989), 75–139, Cambridge Univ. Press, 1991.

[5] A. Fröhlich *Tame representations of local Weil groups and of chain groups of local principal orders*, Sitz. Heidelb. Akad. Wiss. (Mathematik) (1986) (3), 75–170.

[6] P. Gérardin, P. Kutzko *Facteurs locaux pour $GL(2)$*, Ann. Sci. Éc. Norm. Sup. **13** (1980), 349–384.

[7] G. Henniart *Galois ε-factors modulo roots of unity*, Invent. Math. **78** (1984), 117–126.

[8] B. Kahn *Sommes de Gauss attachées aux caractères quadratiques de petit conducteur*, Groupe d'Étude d'Analyse Ultramétrique, Publ. Math. Univ. Paris VII **29**, Univ. Paris VII, 1987, 55–66.

[9] B. Kahn Lettre à G. Henniart, 1er août 1986.

[10] H. Koch *Extendible functions*, prépublication, Edmonton, 1990, 27 pp.

[11] G. Laumon *Transformation de Fourier, constantes d'équations fonctionnelles et conjecture de Weil*, Publ. Math. IHÉS **65** (1987), 131–210.

[12] J. Martinet *Character theory and Artin L-functions*, *in* Algebraic number fields : L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), 1–87, Academic Press, 1977.

[13] J.-P. Serre Représentations linéaires des groupes finis (2ème édition), Hermann, 1971.

[14] J. Tate *Fourier analysis in number fields and Hecke's zeta functions*, thèse de doctorat, Princeton, 1950, reproduite *in* Algebraic number theory (J.W.S. Cassels, A. Fröhlich, eds), Acad. Press, 1967, 305–347.

[15] J. Tate *Local constants*, Prepared in collaboration with C. J. Bushnell and M. J. Taylor, *in* Algebraic number fields : L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), 89–131, Academic Press, 1977.

[16] A. Volf *Sur une conjecture de Deligne et Henniart sur les constantes locales d'équations fonctionnelles des fonctions L*, An. Stiint. Univ. Al. I. Cuza Iasi. Mat. (N.S.) **42** (1996), 239–272 (1998).

[17] A. Volf *Sur le comportement, par torsion, des facteurs ε*, Scr. Sci. Math. **1** (1997), 271–312.

---

28 juillet 2011

Bruno Kahn, Institut de Mathématiques de Jussieu, UPMC - UFR 929, Mathématiques, 4 Place Jussieu, 75005 Paris, France • *E-mail :* kahn@math.jussieu.fr